LONDON FIRE BRIGADE

London Fire Brigade Headquarters
169 Union Street London SE1 0LL
T 020 8555 1200 F 020 7960 3602
Textphone 020 7960 3629
london-fire.gov.uk

Freedom of Information request reference number: FOIA3584.1

Date of response: 27 February 2018

Request and Response:

1. *Does your organisation adhere to the Network Security guidance outlined by the National Cyber Security Centre, within its '10 Steps to Cyber Security'?*

2. *Do you ensure that security patches for critical vulnerabilities are routinely patched within 14 days, as recommended by the National Cyber Security Centre?*

3. *Have you suffered from any service outages on your network in the last two years, however small?*

4. *Did any of these outages cause a loss, reduction or impairment to your organisation's delivery of essential services?*

5. *Was the root cause of the service outage identified and confirmed – at the time or afterwards?*

6. *Is it possible that any service outages you have suffered in the last two years was caused by a cyber attack – such as ransomware, DDoS attack, or malware?*

7. *Are you aware that Distributed Denial of Service (DDoS) attacks are a significant contribution to service interruptions, outages and downtime?*

In response, having reviewed and discussed your request with our ICT department, I can neither confirm nor deny whether the Authority holds the information being requested. This is because under section 24 of the FOIA - National Security disclosing whether or not we hold any of the information being requested would or would be likely to, prejudice the purpose of safeguarding national security.

Whilst section 1(1)(a) of the FOIA requires a public authority to confirm whether it holds the information that has been requested, Section 24(2) provides an exemption from this duty as it states:

'The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.'

Although the s.24 exemption applies, this is not an absolute exemption and the Authority is required to consider a public interest test. This requires us to consider whether the public interest in withholding the information outweighs the public interest in disclosure. I have set out our public interest test considerations for and against disclosure below:

Considerations supporting disclosure:

- the public's right to information held by public authorities.
- disclosure would be consistent with government aims to improve accountability and transparency in the operation of public organisations.
- it could be argued there is a public interest in the disclosure of information on cyber security, hacking and other computer-related attacks as it would provide the public with assurance that the Authority's IT systems are protected appropriately.

Considerations against disclosure:

- Whilst the public has a right to know that IT systems are secure from any external threats, any steps the Authority may or may not be taking to enhance this security should not in the public domain as this might weaken those security measures.
- Disclosing details of any security breaches the Authority may or may not have had, may undermine our ability to secure our information and systems and this may harm our ability to secure the safety and security of the citizens and visitors of London and would not be in the public interest.
- To confirm the details of any successful attacks may provide useful information to anyone planning to attack the Authority's systems. Furthermore the publication of any details of methods in place to stop similar or new attacks, may facilitate further or continued attacks.
- It would not be in the public interest to disclose information that may undermine public safety or undermine law enforcement colleagues thereby assisting those who are intent on endangering national security or threatening the safety and security of the citizens and visitors to London.

I therefore conclude that the public interest in maintaining this exemption and neither confirming nor denying that we have or have not received any attacks and the steps we have or do not have in place to combat these attacks outweighs the public interest in disclosure of the information requested should we hold it. I believe that, should the Authority hold the information you have requested, confirmation or denial of the information would, or would be likely to, prejudice any ongoing work that may be taking place to enhance our systems and defend them from attack.

I'm sorry I cannot be more helpful on this occasion. However I do hope you understand our position.